

Use Well-Known Cryptography Appropriately and Correctly

William L. Fithen, Software Engineering Institute [vita³]

Copyright © 2005 Carnegie Mellon University

2005-10-03

Failing to use, or inventing your own, cryptography can introduce vulnerability.

Description

The following are frequent misuses of cryptography:

- Poor source of random numbers for a cryptographic algorithm.
- Not managing key material safely.
- Attempting to hide cryptographic credentials in client software or on client systems.
- Use of homegrown cryptographic algorithms.
- Use of homegrown implementation of well-known cryptographic algorithms.

References

- [Anderson 93] Ross Anderson. *Why Cryptosystems Fail*.
<http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/wcf.pdf> (1993).
- [McArdle 01] Lorah McArdle. *Beyond Encryption*.
<http://www.sdmagazine.com/documents/s=818/sdm0101i/> (2001).
- [Menezes 96] Menezes, Alfred J.; Van Oorschot, Paul C.; & Vanstone, Scott A. *Handbook of Applied Cryptography*. CRC Press, 1996.
- [Morar 00] Morar, John F. & Chess, David M. *Can Cryptography Prevent Computer Viruses?* <http://www.research.ibm.com/antivirus/SciPapers/VB2000JFM.htm> (2000).
- [Schneier 96] Schneier, Bruce. *Why Cryptography Is Harder Than It Looks*.
<http://www.schneier.com/essay-037.pdf> (1996).
- [Schneier 98] Schneier, Bruce. "Cryptographic Design Vulnerabilities." *Computer* 31, 9 (1998): 29-33.

SEI Copyright

Carnegie Mellon University SEI-authored documents are sponsored by the U.S. Department of Defense under Contract FA8721-05-C-0003. Carnegie Mellon University retains copyrights in all material produced under this contract. The U.S. Government retains a non-exclusive, royalty-free license to

3. file:///portal/vitae/william_l_fithen

publish or reproduce these documents, or allow others to do so, for U.S. Government purposes only pursuant to the copyright license under the contract clause at 252.227-7013.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For inquiries regarding reproducing this document or preparing derivative works of this document for external and commercial use, including information about “Fair Use,” see the [Permissions](#)¹ page on the SEI web site. If you do not find the copyright information you need on this web site, please consult your legal counsel for advice.

Felder

Name	Wert
Copyright Holder	SEI

Felder

Name	Wert
is-content-area-overview	false
Content Areas	Knowledge/Guidelines
SDLC Relevance	Implementation
Workflow State	Publishable

1. <http://www.sei.cmu.edu/about/legal-permissions.html>